REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
Nov 2010		

4. TITLE AND SUBTITLE

Information Assurance and Cyber Defence
(Assurance de l'information et cyberdéfense)

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Research and Technology Organisation (NATO)
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Research and Technology Organisation (NATO)
BP 25, F-92201 Neuilly-sur-Seine Cedex, France

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

RTO-MP-IST-091

12. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES

Supporting documents are attached to the report as separate files (MS Word, PDF, HTM).

14. ABSTRACT

The broad use of information and communication technology in information warfare makes NATO's critical IT infrastructure its most valuable asset and its most vulnerable point of attack. Military platforms are becoming more computer intensive, which means that software is becoming more complex and taking on larger and more important roles, and information systems are being increasingly interconnected, which means that vulnerability in a single program can put an entire infrastructure at risk. As a consequence, information systems security and defense against cyber attacks are major issues and major concerns, especially in joint/coalition operations. Finding effective ways to protect and defend information and information systems by ensuring their availability, integrity, and confidentiality is challenging even with the most advanced technology and trained professionals.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
U	U	U	SAR	13	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

NORTH ATLANTIC TREATY ORGANISATION

RESEARCH AND TECHNOLOGY ORGANISATION

AC/323(IST-091)TP/328

www.rto.nato.int

RTO MEETING PROCEEDINGS **MP-IST-091**

Information Assurance and Cyber Defence

(Assurance de l'information et cyberdéfense)

Papers presented at the Information Systems and Technology Panel (IST) Symposium held in Tallinn, Estonia, 22 - 23 November 2010.

Published November 2010

The Research and Technology Organisation (RTO) of NATO

RTO is the single focus in NATO for Defence Research and Technology activities. Its mission is to conduct and promote co-operative research and information exchange. The objective is to support the development and effective use of national defence research and technology and to meet the military needs of the Alliance, to maintain a technological lead, and to provide advice to NATO and national decision makers. The RTO performs its mission with the support of an extensive network of national experts. It also ensures effective co-ordination with other NATO bodies involved in R&T activities.

RTO reports both to the Military Committee of NATO and to the Conference of National Armament Directors. It comprises a Research and Technology Board (RTB) as the highest level of national representation and the Research and Technology Agency (RTA), a dedicated staff with its headquarters in Neuilly, near Paris, France. In order to facilitate contacts with the military users and other NATO activities, a small part of the RTA staff is located in NATO Headquarters in Brussels. The Brussels staff also co-ordinates RTO's co-operation with nations in Middle and Eastern Europe, to which RTO attaches particular importance especially as working together in the field of research is one of the more promising areas of co-operation.

The total spectrum of R&T activities is covered by the following 7 bodies:

- AVT Applied Vehicle Technology Panel
- HFM Human Factors and Medicine Panel
- IST Information Systems Technology Panel
- NMSG NATO Modelling and Simulation Group
- SAS System Analysis and Studies Panel
- SCI Systems Concepts and Integration Panel
- SET Sensors and Electronics Technology Panel

These bodies are made up of national representatives as well as generally recognised 'world class' scientists. They also provide a communication link to military users and other NATO bodies. RTO's scientific and technological work is carried out by Technical Teams, created for specific activities and with a specific duration. Such Technical Teams can organise workshops, symposia, field trials, lecture series and training courses. An important function of these Technical Teams is to ensure the continuity of the expert networks.

RTO builds upon earlier co-operation in defence research and technology as set-up under the Advisory Group for Aerospace Research and Development (AGARD) and the Defence Research Group (DRG). AGARD and the DRG share common roots in that they were both established at the initiative of Dr Theodore von Kármán, a leading aerospace scientist, who early on recognised the importance of scientific support for the Allied Armed Forces. RTO is capitalising on these common roots in order to provide the Alliance and the NATO nations with a strong scientific and technological basis that will guarantee a solid base for the future.

Published November 2010

ISBN 978-92-837-0115-6

Information Assurance and Cyber Defence

(RTO-MP-IST-091)

Executive Summary

Information Assurance and Cyber Defence represent a broad domain, this Symposium addresses some of the research topics in this field which are regarded as important; not only scientifically, but also operationally and politically. Progress is reported in the disciplines of:

- Intrusion Detection, Protection and Countermeasures;
- Security Models and Architectures;
- Security Policies, Evaluation, Authorisation and Access Control; and
- Network and Information Security Awareness.

Various projects, both national and with international collaboration, are discussed in the proceedings of the Symposium. Progress described is significant with some mechanisms able to detect abnormal behaviour confirmed through experimentation. Of interest is the detection of bots; current methods achieving some success by applying Genetic Algorithms, it is hoped that detection will be more readily achieved in the near future. Transfer of information about a potential threat particularly across national boundaries eases the situation and brings together a diversity of surveillance techniques. Establishing mutual trust is paramount to achieve a timely reaction with schema described to improve confidence. The installation of dedicated CERT (Computer Emergency Response Teams) has shown merit in Poland and should be considered elsewhere. A potential solution to ease security by employing the necessary and sufficient core of open systems enhanced by weaving in additional security features is advocated and looks encouraging. A main threat to systems remains the disillusioned system operator who is able to bypass a number of the security features.

Several papers address the PCN (Protected Core Network) concept which appears to be viable. An exercise/ experiment was conducted in the Baltic which was successful in showing the principles and is reported in the proceedings. A warning about RFIDs and simple wireless devices is included describing the vulnerability of systems to replication of bugs which will corrupt the data and allow attackers to set up false nodes.

A proactive stance to predict the next generation of threats is advocated and use of Genetic Algorithms thought appropriate. The mathematics of this discipline are sufficiently advanced that some confidence is generated in the predictions and several groups have the expertise to select the evolutionary process.

The heavy reliance on software in both military and civilian systems leaves the users vulnerable to cyber attack. Whilst the defender has the benefit of knowing his system the attacker has leverage in that a small resource can cause major disruption and hence vigilance by all users is required. The proceedings include papers by the invited speakers addressing observations of attacks and good practice to limit the impact of such attacks. The Symposium proceedings provide a considered assessment of the subject and identify areas where further research would be beneficial.

Assurance de l'information et cyberdéfense

(RTO-MP-IST-091)

Synthèse

L'assurance de l'information et la cyberdéfense représentent un vaste domaine, et ce symposium aborde certains thèmes de recherche de ce domaine considérés comme thèmes majeurs ; non seulement d'un point de vue scientifique, mais également d'un point de vue opérationnel et politique. On note des progrès dans les disciplines suivantes :

- Détection d'intrusion, protection et contre-mesures ;
- Modèles et architectures de sécurité ;
- Politiques de sécurité, évaluation, agrément et contrôle d'accès ; et
- Sensibilisation à la sécurité du réseau et de l'information.

Plusieurs projets d'envergure nationale et internationale sont traités dans les actes du symposium. Les progrès décrits sont significatifs, avec des mécanismes capables de détecter un comportement anormal confirmé grâce à l'expérimentation. La détection de « bots » est particulièrement intéressante ; les méthodes actuelles ayant obtenu certains résultats grâce à l'application d'algorithmes génétiques, nous espérons que la détection atteindra un niveau de maturité technologique plus élevé dans un futur proche. Le transfert d'informations concernant une menace potentielle, par-delà les frontières nationales, facilite la situation et rassemble diverses techniques de surveillance. L'établissement d'une confiance mutuelle est crucial pour obtenir une réaction rapide selon le schéma décrit et visant à améliorer la confiance. L'installation de CERT dédiées (Equipes d'intervention en cas d'urgence informatique) a prouvé leur utilité en Pologne et doit être envisagée ailleurs dans le monde. Une solution potentielle est préconisée et paraît encourageante : elle consiste à faciliter la sécurité grâce à une utilisation fondamentale et suffisante du cœur des systèmes ouverts, améliorés par le maillage de dispositifs de sécurité additionnels. La principale menace envers les systèmes demeure l'opérateur système déçu et capable de contourner un certain nombre de dispositifs de sécurité.

Plusieurs articles traitent du concept du RCP (Réseau central protégé) qui apparaît comme une option viable. L'exercice/expérience menée en mer Baltique en a démontré les principes avec succès et est décrite dans les actes du symposium. Un message d'avertissement concernant l'identification par radio-fréquence (RFID) et les dispositifs simples sans fil est inclus au travers d'une description de la vulnérabilité des systèmes face à la réplication des bogues qui corrompent les données et permettent aux agresseurs de mettre en place de faux nœuds.

Il est recommandé d'adopter une approche proactive visant à prévoir la prochaine génération de menaces, et l'utilisation d'algorithmes génétiques est jugée appropriée. Les mathématiques de cette discipline sont à un niveau suffisamment avancé pour générer une certaine confiance dans les prévisions et plusieurs groupes possèdent l'expertise requise pour sélectionner un processus évolutif.

La grande dépendance à l'égard des logiciels dans les systèmes civils et militaires rend les utilisateurs vulnérables aux cyberattaques. Tandis que le défenseur a l'avantage de connaître son système, l'agresseur possède la force, car une toute petite ressource peut être à l'origine de perturbations majeures, et il est par conséquent important que tous les utilisateurs fassent preuve de vigilance. Les actes comprennent des articles écrits par les intervenants invités décrivant les observations d'attaques et les bonnes pratiques à respecter pour limiter l'impact de telles agressions. Les actes du symposium fournissent une évaluation minutieuse du sujet et identifient les domaines où des recherches approfondies s'avèreraient utiles.

Technical Evaluation Report

INTRODUCTION

This report addresses the IST-091 Symposium on Information Assurance and Cyber Defence held on the 22nd and 23rd November 2010 in Tallinn; rescheduled from the 26th and 27th April 2010. A welcome speech by the Estonian Minister of Defence Dr Jank Aaviksoo emphasised the importance of the topics addressed at the symposium particularly when he coupled the disciplines with those discussed at the summit in Lisbon, which he had attended the previous week. The symposium was divided into four session addressing:

- Intrusion Detection, Protection and Countermeasures
- Security Models and Architectures
- Security Policies, Evaluation, Authorisation and Access Control
- Network and Information Security Awareness

The topics for the symposium had been established sometime ago and the papers reflected the further research which had taken place following the postponement caused by air transport disruption resulting from the Icelandic Ash Cloud. The topics included in the Call for Papers were appropriate and reflected the wide domain covered by the title. Not all the topics solicited a response, of note were detail of cryptographic protocols, key management and recovery, insider attack counters and trust negotiations. It is recognised that some of these topics may be sensitive but dissemination of information is critical to cyber defence which is not restricted to the military.

Initially, in April, 58 abstracts were received and a commendable programme of 28 presentations and 15 poster sessions were identified. The papers submitted in April were generally of a high standard and it is regrettable that the ash cloud forced a postponement. The reorganised event attracted about fifty percent of the original response and in some instances the technical committee members were unable to attend, which was disappointing, but understandable. Despite the enforced rescheduling this symposium has been a success and the symposium chair Prof. Nazife Baykal and her technical committee should be congratulated on their persistence to retain the quality and enthusiasm.

ISSUES

All IT systems whether military or civilian are subject to threats which are not static. The impact on some control systems e.g. power stations could be catastrophic if sustained attacks are successful.

Hackers are becoming more sophisticated, see the challenge of Stuxnet.

Botnets are becoming more prolific

Transfer of Cyber information and knowledge needs improving both in quality and timeliness, this requires trusted communications.

The vocabulary of the discipline needs to be consistent for all the users; see use of an ontology.

DISCUSSION

Cyber Defence is a broad church well beyond strictly military applications but the principles are very similar to conventional warfare. The process is well known and follow:

a) Detect a threat;

b) Identify the threat;

c) Take timely action to reduce the effect; and

d) Secure safe recovery of the system under attack.

Regrettably the dynamic nature of the potential threats demands a proactive stance to ensure that appropriate counters are available.

It was pleasing to note that the welcome speech by the minister aligned the topics discussed at the summit with those of the symposium. The papers, in the symposium, were topical and generally of a high standard addressing the issues identified above. Progress was significant with some mechanisms able to detect abnormal behaviour; detection of bots was indicated but was processor intensive. Transfer of information about a potential threat particularly across national boundaries with the appropriate trust was deemed necessary for a timely reaction. The installation of a dedicated CERT team has shown merit in Poland and should be consider elsewhere.

Security using open systems enhanced by weaving in additional security features looks encouraging. SCADA systems should be made robust with the use of security tokens and adding necessary signatures in data partitions to hamper intruders.

Several papers addressed the PCN (Protected Core Network) concept which appears to be viable. An exercise/experiment was conducted in the Baltic which was successful in showing the principles. A warning about RFIDs and simple wireless devices was made since they are declared vulnerable to replication of bugs which will corrupt the data and allow attackers to set up false nodes with the consequential outcome.

A proactive stance to predict the next generation of threats was advocated and use of Genetic Algorithms thought appropriate. The mathematics of this disciple are sufficiently advanced that some confidence is generated in the predictions.

DETAIL OF THE PAPERS

The first invited speaker, Geer from the Cooperative Cyber Defence Centre of Excellence Estonia, provided a background with an assessment of the observed attacks and the capabilities of a small group of attackers. The emphasis of the presentation was on hacking but he readily acknowledged that hacking was only a small part of the problem. The historical examples which he provided showed considerable gearing, in favour of the adversary. with massive disruption caused by limited resources. The defender does, however, have an advantage in a reactive posture with knowledge of the platform he is defending. He highlighted the example of malware hidden in MP3 formats but indicated that the biggest weakness of the systems is to prevent disaffected internal users corrupting systems. This group will hold security privileges allowing them to bypass a number of the security features. I was a little disappointed with the lecture and thought that greater detail of the current problems could have been aired.

Rumour Detection in Information Warfare: Understanding Publishing Behaviours as a Prerequisite was the first submitted paper presented by Nel. The need for rumour detection was emphasised because of the ease in which publications on the internet can be manipulated. A detection process was presented in which changes in published material and behaviours were identified for analysis. The tool ONICS (Ontils de Navigation,d'Indexation et de Classement des Sources) was described which combines hierarchal clustering and 'k-mean' to extract the clusters of common behaviour. It is known that this method is computationally demanding. Some initial results were presented which showed that multiple patterns

could be identified with a consensus matrix. The work used known publishing houses e.g. Le Monde for its source data. Further work would benefit by applying other descriptors and to establish the propagation mechanism.

A second paper on behavioural analysis this time by Gates entitled Combining Trust and Behavioural Analysis to Detect Security Threats. The current methods suffer from a declared high false alarm rate and leads to a low degree of confidence in the results. The proposal presented was to establish the aggregated behavioural space by the dynamic use of ontologies. Basic SiLK data was employed to display patterns establish from selecting the ordinate and abscissa using heuristics. The technique can be compared to methods adopted to extracting signals in an ESM domain. Several results were presented which isolated clusters for further analysis and inference. The results clearly show temporal aspects and country of origin as significant.

Couture presented a paper on 'Using Anticipative Malware Analysis to Support Decision Making' which advocated the use of an encyclopedia holding the parameters of an attack. The design of a support tool is in progress and a demonstration was offered, it shows promise but has some limitations. It will search internet addresses and report on the activities of the malware. A degree of filtering is necessary to limit the time required for analysis. A question from the floor was posed on the capability when faced with block communications.

Extending Mondrian Memory Protection was presented by Kolbitsch as part of multinational cooperation. The memory management scheme was developed to identify race conditions to retain a stable and secure memory. The basis of the work was the x86 memory management with the inherent coarse control limited to two bits. This was then compared with the standard Mondrain implementation before discussing the extended Mondrian Memory eMMP. This has a user defined access with fine grain protection,the claim is that it will identify race conditions.

Inan presented 'Information Security in Maritime Domain Awareness';he described the process to acquire information superiority which relies on secure exchange. The system employs an air gap between the secure and unclassified domains. The alternative use of a virtual air gap was indicated but the details were not available but see following paper also from Turkey

Virtual Air Gap: A Secure Architecture for Information Assurance by Ozgit. The virtual air gap is a mechanism which allows information to flow across the boundary without IP connectivity. This is achieved by both sides accessing a common data base. The design is the subject of a patent application with software development in progress. The security is enforced with a crypto function where the keys are stored external to the system. It will currently handle a throughput of 20Mbps with a delay of 10nsec. The longterm aim is to handle video streaming. No formal analysis was evident.

Coalition Network Defence. Common Operational Picture by Tolle. This was a presentation outlining the work of task group IST-081/RSG-039 sponsored by the IST panel. The aim of the group is to investigate how sharing cyber defence information can enhance global situational awareness. It is foreseen that a number of the current challenges will be resolved particularly in the area of legal ownership and the procedural implications. The COP will then incorporate Threat Intelligence, Malware Analysis and Risk Assessment

Goranin then presented a paper from Lithuania entitled Extension of the Genetic Algorithm Based Malware Strategy Evolution Forecasting Model for Botnet Strategy Evolutionary Modeling. The paper focuses on the proactive approach by understanding the evolutionary trends in malware development. It has been shown that botnets will exhibit the characteristics curve for propagation as that for epidemics with different time scales and peak infection values. The design aim is to force the malware to saturate as soon as possible with a low value for the saturation. Genetic Algorithms(GA) emulate the natural

environment and their use offers a measure of forecasting The model appears to be in an advanced state but needs real statistical data for parametric training.

Couture presented a critical overview on 'Self Defence of Information Systems in Cyber-Space. He discussed the strategy, based on good system concepts of redundancy and diversity. The conceptual architecture used LINUX and BSD UNIX for diversity in a redundant configuration. The operating systems were at the core with controllers and comparators linked to ensure consistency, in this mode any probe would need to solicit the same response in the same time frame for both systems; regarded as unlikely. The system would have health assessment with embedded forensics capture and thus have a potential life of some 20 years. A question from the floor raised the issue of using virtual machines to establish redundancy.

The second morning started with the second of the invited keynote speakers. Corcoran gave a lecture on 'The Way Forward Following The Strategic Defence Review' He identified the issues of cyber defence applicable to a multinational group but developed from a UK perspective. Whilst the cyber threat is difficult to define, because of the evolving and transient nature, all the evidence points to a growing risk. Attacks on secondary installations can be devastating and pose a major economic risk. Tier 1 threats were declared all the counters indicate a desire for stronger international alliances to ensure fragmented intelligence is coupled. The need to enhance research was raised and again improve the derived information. The question of targeting econometrics was indicated together with the implied impact on the population. The structure of the internet specifically designed as an open system permits the inclined adversary to reroute all traffic through selected servers for potential analysis; examples are available. Action is necessary before the general population are effected though critical events e.g. power failures or financial instability. The lecture provided a reasoned appraisal of the environment and should encourage a proactive posture through research and information exchange.

Metrics based Computer Network Defence Decision Support by Sawilla was the next presentation. The approach was to exploit the field of graph theory to analyse the networks. The graph constructed uses AND nodes for compound dependences and OR nodes for redundancy, a further constraint is to complete the analysis and offer solutions in a short time frame consistent with the rate of change of the network. Some graphs have been constructed and the results are encouraging. A comment from the floor confirmed that speed is essential with recommendation provided before an optimum solution is provided.

Besson gave a presentation based on work in Thales on 'Developing a Cooperative Intrusion Deception System for Wireless Sensor Networks.' The presentation was a description of the AWISSENET project within the European Framework Initiative, with the aim to develop a security toolbox for trusted routing, service discovery and intrusion detection in WSNs. The issue is one where a large number of simple devices are deployed and the information gathered in a central processor. They are used both by the military and industry and were shown to be vulnerable. Most devices are power limited with the consequential minimal functionality allowing false signals to be injected or false nodes can be add to the network. The counter is to add a level of security through the use of secure protocols and voting methods but this will inevitably be power consuming and hence detract from the primary purpose.

Schutz again from Thales presented 'Protecting Core Networks Concepts and Changes'. This was selected as a poster session in April but allocated for presentation at this symposium. The concept of a local protected core was expanded to cover multinational and NATO deployments. The use of enforcement nodes interfacing with the coloured clouds representing different levels of classification has been expanded. The degree of diversity was discussed during questioning.

A second paper by Gates was presented on FloVis: Leveraging Visualisation to Protect Sensitive Network Infrastructure. The tool presented is extremely powerful in giving a wide spectrum and perspective to the data collected. Standard views are available but the skill and experience of the analyst is necessary to drill

down to the appropriate data set. The aspect of how the necessary and sufficient data reaches the repository for analysis was a little vague, examples of SiLK data were presented. The IST have sponsored an independent research study group in this discipline, the inclined reader is directed to their report for additional detail.

Validation of the PCN Concept: Mobility, Traffic Flow Confidentiality and Protection Against Directed Attacks was presented by Carlen. The paper presented some experimental results for an environment around the Baltic. It reports on the work of the RTG-032 Task Group sponsored by IST. In general it proved the PCN concept but identified some areas for improvement, particularly in the peer-peer discovery following CC movement. During the exercise 8 out of 9 of the PCNs regained communications within 2 minutes following relocation. The enforcing nodes used open source IP sec routing on a LINUX Ubuntu server.

Silick from Poland presented ' Research and Development Projects Launched in Response to the Dynamic Evolution of Internet Security Threats- A Perspective of a CERT Team' . Computer Emergency Response Teams (CERT) have been established to provide a first response to internet security incidents. The presentation covered four related projects ARAKIS, Honey Spider, Wombat and Fisha some of which had received funding from the EU. Arakis detects threats through scanning by aggregating data from distributed sources . Honey Spider has been designed to counter browser exploits and serves as an early warning. Wombat expands the monitoring to a global scale in conjunction with other agencies whilst Fisha concentrates on the European environment to alert small business of a threat. A conclusion from the project is that knowledge exchange in a timely fashion is highly significant.

Authentication and Authorisation of Users and Services in Federated SOA Environments – Challenges and Opportunities was presented by Jasiul again from Poland. The motivation for this project was to ensure trusted information exchange to establish a Coalition Common Operational Picture, but is also loosely coupled with the paper above. The exchange is achieved with a federated system having a trusted interface at the PEP level. A multinational exchange was created to exercise the principles using SAML(Security Assertion Markup Language) and PKI (public key infrastructure); some issues were identified and solutions implemented.

Kiviharju presented 'RFID as a Tool in Cyber Warfare'. A warning was given that despite the small memory size of most RFIDs, malware can propagate and contaminate the TAG. A case study is available for inspection in the paper, the mechanism is by self replication onto the data base. Since RFIDs are employed in logistic systems care should be exercise in their deployment.

Security Evaluation and Hardening of FOSS was a second paper presented by Charpentier. Trusted free and open source software (FOSS) has been available for some time and has been used in the military since about 2005. A strong recommendation from the presenter was that a hybrid of COTS and FOSS can be beneficial. The paper offers a mechanism to establish secure software; he takes FOSS removes unnecessary code and adds ad hoc security functions. The weaving of FOSS and specific code is undertaken at an intermediate level. In the examle presented this was undertaken in GIMPLE.

Strategic Road Map of Network Enabled Capability for Defence in Turkey by Arslan. As the title implies this presentation was the Turkish perspective of implementing NEC with the appropriate security features.

The final paper 'Automated Attacker Correlation for Malicious Code' was presented by Dullen. The amount of malware is rapidly increasing and automatic methods are required to identify events and incidents which will cause harm. The paper describes VxClass which detects similarities between executables. This is achieved by unpacking the engine, use a fast comparator to establish clusters and hence isolate the signature. Details of the elements are available in the paper together with a case stude undertaken within the financial sector. The presentation also offered a means of breaking the cycle by partitioning the users data base and giving each group a different signature.

ROUND TABLE DISCUSSION

The discussion was subdivided into a Political focus followed by a Technical focus.

Political Focus

A short presentation was given by Anil who is Head, Cyber Defence at NATO HQ, he outlined the Emerging Security Challenges Division (ESCD) and outlined the way ahead on Cyber Defence discussed at the recent summit in Lisbon. The political statements appear to reflect the aims of the symposium. A copy of the statement applicable to Cyber Defence is available in Anil's slides.

Technical Focus

To set the scene for discussion Grosche presented a view starting from the OODA loop. He posed the rhetorical question as to how to gain in depth knowledge of the malware and used Conficker and Stuxnet as examples to counter. The need to liaise with coalition partners to share information of an attack became obvious as the threats became widespread.

A lively discussion ensued with elaboration on Genetic Algorithms and Botnets. General agreement was reach consisted with the detail presented during the symposium. It was acknowledged that the transfer of information is a cultural aspect and in some instances better protection would be afforded when the legal and political constraints are removed.

ANALYSIS OF QUESTIONNAIRES

I received 34 replies to the questionnaires which is about a third of the registered attendance. From experience extremes of the population will voice an opinion so we can assume we have a representative sample. Not all the returns had all the questioned answered.

All the returns indicated that the symposium was well organised.

60% thought the theme very appealing; 40% satisfactory

60% thought the symposium worthwhile; 38% sufficient and one replied as partial

5 replies though that the papers met half the objectives; all others thought that most papers were compliant.

For the overall impression 26% Excellent 60% Very Good and 14% Good

94% marked the overall value in excess of 81 with one at 61-70 and one at 71-80

The selection of the most interesting and least interesting papers are reasonably spread reflecting the disciplines of the audience

I received one adverse comment relating to the way that the session chairs introduced the speakers, he thought that the CV could be compressed.

CONCLUSIONS

The symposium has addressed a wide number of issues within Cyber Space and provided a forum to disseminate information in an informal manner. The coffee breaks and lunch times afforded an

environment conducive for networking and establishing trust to subsequently transfer knowledge. The timely transfer of information particularly across national boundaries has been advocated throughout the symposium. Research topics were aired which progress the knowledge in the Cyber Defence field but further work is necessary to preempt the next generation of threats. Attackers are becoming more sophisticated aided by advances in technology and the proliferation of simple devices which can propagate bugs.

I am pleased to conclude that the symposium was well organised, addressed pertinent issues and was of a high quality.

Glyn Wyman

TER IST-091